UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/988,009	11/16/2001	James De Perna	067389-0023	7685

20277 7590 07/24/2008

MCDERMOTT WILL & EMERY LLP
600 13TH STREET, N.W.
WASHINGTON, DC 20005-3096

EXAMINER	
ZIA, SYED	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
07/24/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/988,009	PERNA ET AL.	
	Examiner	Art Unit	
	SYED ZIA	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 April 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,6-52,54-59 and 61* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,6-52,54-59 and 61* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *01/2008*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

This office action is in response to amendments and remarks filed on April 28, 2008. Original application contained Claims 1-50. Applicant previously amended Claims 1, 3, 5-7, 11, 16, 19-20, 25, 33, 39, 41-50, 58, 60, and added new Claims 51-60. Applicant currently amended Claims 1, 25, 41, 54, 54, cancelled Claim 53, and added new Claim 61. The amendments filed on April 28, 2008 have been entered and made of record. Presently Claims 1-4, 6-52, 54-59, and 61 are pending for consideration.

Response to Arguments

Applicant's arguments filed on April 28, 2008 have been fully considered but they are not persuasive because of the following reasons:

Regarding Claims 1, and 41 applicants argued that the system of cited prior art (CPA) [Yaung et al. (U. S. Patent No. 6,446,069] do not specifically teach that fails to specifically describe *"applying a dual hierarchical safeguard on both (1) functions of software applications and (2) data that access by users are to be guarded and controlled, such that an entitlement of a user to one of the hierarchically arranged functions automatically applies to functions that are*

hierarchically subordinate to the one of the plurality of hierarchically arranged functions, and an entitlement of access the hierarchically arranged data automatically grants access to all the data that are hierarchically subordinate to the level granted to the user,", as recited in independent claim 1.

This is not found persuasive. The system of cited prior art teaches system that relates to user access control method that involves restricting access by users to functions based on whether user has been associated with application privileges for function by using an extensible application-specific access control model, and an Object-Oriented Application Program Interface (API) design implementing the model. The extensible application-specific access control model allows each application program to define its privileges using an extensible application-specific privilege vector within the digital library (col. 6 line 30 to col.10 line 64).

As a result, cited prior art does implement and teach system and method that relates to an application for protecting software applications and their underlying proprietary data.

Applicants still have failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts.

Therefore, the examiner asserts that cited prior art does teach or suggest the subject matter broadly recited in independent and dependent claims. Accordingly, rejections for Claims 1-4, 6-52, 54-59, and 61 are respectfully maintained.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-4, 6-52, 54-59, and 61 are rejected under 35 U.S.C. 102(e) as being anticipated by Yaung et al. (U. S. Patent No. 6,446,069).

1. Regarding Claim 1 Yaung teach and describe a system for selectively granting access to the functionality of a software application to a plurality of users, comprising: a first memory configured to store first data related to the software application, and second data specifying entitlements of each of the plurality of users to access a plurality of preset functions of the software application; and a rules checker in communication with the software application and the first memory (col.5 line 58 to line 66, and col.6 line 30 to line 58), said rules checker (i.e. Access Control List ACL) configured to:

receive at least one query, wherein the query is generated in response to an input received from one of the plurality of users with respect to the software application, and forward a message to the software application in response to the query, wherein the message is generated based on the query and the second data, wherein said message provides instructions to the software application regarding entitlements of one of the plurality of users to access at least one of the plurality of preset functions of the software application (col.9 line 1 line 1 to col.10 line 11);

the first memory stores the respective first data for each software application including an identification of hierarchically arranged functions associated with that software application (col.7 line 35 to line 59); and an entitlement of one of the plurality of users to one of the hierarchically arranged functions automatically applies to functions that are hierarchically subordinate to the one of the plurality of hierarchically arranged functions, according to the respective first data stored in the first memory(col.9 line 26 to col.10 line 12);

the one of the users is an organization having associated proprietary data; the second data includes an assigned access level to access the proprietary_ data by an individual user within the organization, wherein the assigned access level is selected from among a plurality of access levels arranged in a hierarchical structure, and specifies an authorization to access at least part of the proprietary_ data associated with the organization;

the assigned access level allows access to all data accessible to all access levels hierarchically subordinate to the assigned access level; and

when the individual user utilizes one of the software applications to process the proprietary data, the assigned access level of the individual user and an assigned entitlement of the individual user to one of the hierarchically arranged functions determine available functions of the one of the software applications and available proprietary data to the individual user (col. 6 line 30 to col.10 line 64).

2. Regarding Claim 25, Yaung disclose a method for providing application-level security, said method comprising the steps of: storing first data relating to a software application; storing second data specifying entitlements of each a plurality of users to access a plurality of preset

functions of the software application (col.5 line 58 to line 66, and col.6 line 30 to line 58), receiving a query, wherein the query is generated in response to an input from one of the plurality of users with respect to the software application; in response to the query, forwarding a message to the particular software application, said message being generated based on the second data and the query, and providing instructions to the particular software application regarding entitlements of the one of the plurality of users to access at least one of the plurality of preset functions of the software application(col.9 line 1 line 1 to col.10 line 11)

wherein:

the respective first data for each software application includes an identification of hierarchically arranged functions associated with that software application;

an entitlement of the one of the plurality of users to one of the hierarchically arranged functions automatically applies to functions that are hierarchically subordinate to the one of the plurality of hierarchically arranged functions, according to the respective first data stored in the first memory:

the one of the users is an organization having associated proprietary data: the second data includes an assigned access level to access the proprietary data by an individual user within the organization, wherein the assigned access level is selected from among a plurality of access levels arranged in a hierarchical structure, and specifies an authorization to access at least part of the proprietary data associated with the organization:

the assigned access level allows access to all data accessible to all access levels hierarchically subordinate to the assigned access level; and

when the individual user utilizes one of the software applications to process the proprietary data, the assigned access level of the individual user and an assigned entitlement of the individual user to one of the hierarchically arranged functions determine available functions of the one of the software applications and available proprietary data to the individual user (col. 6 line 30 to col.10 line 64).

3. Regarding Claim 41, Yaung disclose a computer readable medium bearing instructions for providing application-level security, said instructions being arranged to cause one or more processors upon execution thereof to perform the steps of: in a first memory storing first data relating to a software application; in the first memory, storing second data specifying entitlements of each of a plurality of users to access a plurality of preset functions of the software application (col.5 line 15 to line 66, and col.6 line 30 to line 58); receiving a query, wherein the query is generated in response to an input from one of the plurality of users with respect to the software application; in response to the query, forwarding a message to the software application, said message being generated based on the second data and the query, and providing instructions to the software application regarding entitlements of the one of the plurality of users to access at least one of the plurality of preset functions of the particular software application (col.9 line 1 line 1 to col.10 line 11); wherein

The first memory stores the respective first data for each software application including an identification of hierarchically arranged functions associated with that software application (col.7 line 35 to line 59); and an entitlement of one of the plurality of users to one of the hierarchically arranged functions automatically applies to functions that are hierarchically subordinate to the

one of the plurality of hierarchically arranged functions according the first data stored in the first memory (col.9 line 26 to col.10 line 12);

the one of the users is an organization having associated proprietary data; the second data includes an assigned access level to access the proprietary_ data by an individual user within the organization, wherein the assigned access level is selected from among a plurality of access levels arranged in a hierarchical structure, and specifies an authorization to access at least part of the proprietary data associated with the organization; the assigned access level allows access to all data accessible to all access levels hierarchically subordinate to the assigned access level; and when the individual user utilizes one of the software applications to process the proprietary data, the assigned access level of the individual user and an assigned entitlement of the individual user to one of the hierarchically arranged functions determine available functions of the one of the software applications and available proprietary data to the individual user (col. 6 line 30 to col.10 line 64).

5. Claims 2-4, 6-24, 26-40, and 42 –59 are rejected applied as above rejecting Claims 1, 25, and 41. Furthermore, Yaung teach and describe,

As per claim 2, wherein the first memory is a relational database (col.4 line 51 to line 58).

As per claim 3, wherein the software application is implemented on one of a mainframe and a distributed computing (col.4 line 35 to line 50).

As per claim 4, further comprising: a second memory configured to store proprietary data useful to the particular software application, and wherein said message provides information to

the particular software application regarding authorization to output portions of the proprietary data (col.5line 15 to line 22).

As per claim 6, wherein the query further comprises information relating to the one of the users and relating to at least one of the functions associated with the particular software application, and wherein the message relates to that one user's authorization to access the at least one function (col.8 line 23 to line 45).

As per claim 7, wherein the identification of hierarchically arranged functions include functions, sub-functions, and sub-sub functions (col.7 line 35 to col.8 line 59, and col.10line 55 to line 56).

As per claim 8, wherein the respective first data for each software application includes an identification of data fields associated with that software application (col.7 line 45 to line 60).

As per claim 9, wherein the query further comprises information relating to one of the users and relating to at least one of the data fields associated with the particular software application, and wherein the message relates to that one user's authorization to access the at least one field (col.7 line 45 to line 60).

As per claim 10, wherein the rules checker is further configured to: generate the message based on the query, the first data and the second data (col.9 line 1 to line 25).

As per claim 11, wherein: the respective second data for each of the users includes at least one role, from among a plurality of roles, associated with that particular user, and a description of which of the plurality of roles is entitled to access each of the functions (col.9 line 26 to col.10 line 12).

As per claim 12, wherein: the query includes an identification of a specific one of the users and a specific one of the functions associated with the particular software application; the rules checker is further configured to generate the message based on the query, the first data and the second data; and the message instructs the particular software application regarding that specific user's entitlement to access that specific function (col.9 line 26 to col.10 line 12).

As per claim 13, wherein the rules checker logs data relating to an instance in which the specific user is not entitled to access that specific function (col.9 line 26 to col.10 line 12).

As per claim 14, wherein the respective second data for each of the users includes an access level from among a plurality of access levels, associated with that particular user, said access level determining an authorization of that particular user to access proprietary data within the second memory, and the rules checker is further configured to generate the message based on the query, the first data and the second data (col.8 line 45 to col.10 line 12).

As per claim 15, further comprising: an administrative application configured to facilitate administration of the first and second data (col.6 line 30 to line 57).

As per claim 16, wherein the administrative application is further configured to manipulate the first data according to which of a plurality of clients the plurality of users is associated with (col.6 line 59 to line 65, and col.7 line 9 to line 24).

As per claim 17, wherein the administrative application is further configured to manipulate the first data according to an identity of a particular one of the users (col.7 line 24 to line 35).

As per claim 18, wherein the administrative application is further configured to manipulate the first data according to which of a plurality of roles a particular one of the users is associated with (col.7 line 36 to col.8 line 65).

As per claim 19, wherein the administrative application is further configured to manipulate all the first data relating to a specific one of the software application (col.7 line 36 to col.8 line 65).

As per claim 20, wherein the administrative application is further configured to manipulate all the first data relating to one of a plurality of functions associated with the software application (col.7 line 36 to col.8 line 65).

As per claim 21, further comprising: an auditing application configured to facilitate auditing of the first and second data and any additional data generated by the rules checker (col.7 line 36 to col.8 line 65).

As per claim 22, wherein the auditing application is further configured to provide a history, upon request, of messages forwarded by the rules checker (col.8 line 62 to line 67).

As per claim 23, wherein the history emphasizes those messages related to a failed attempt to access the particular function (col.9 line 26 to line 44).

As per claim 24, wherein the auditing application is further configured to provide a history, upon request, of changes to one or both of the first data and the second data (col.8 line 62 to col.9 line 44).

As per claim 26, further comprising the step of: generating the message based on the query, the first data and the second data (col.7 line 45 to col.8 line 50).

As per claim 27, wherein the query includes an identification of the particular user and the function (col.7 line 60 to col.8 line 27).

As per claim 28, wherein the second data includes for each user, one or more of an associated user ID, client name, role, and business level (col.8 line 45 to col.8 line 67).

As per claim 29, wherein the first data includes for each software application an identification of associated hierarchically arranged functions and characteristics of those users authorized to access each such function (col.7 line 60 to col.8 line 67).

As per claim 30, further comprising the steps of: correlating the first and second data to determine authorized functions, said authorized functions being those particular functions of each software application which are accessible by a specified user; generating the message based on the query and the determination of authorized functions, wherein said query includes an identification of the particular user and the function (col.7 line 60 to col.8 line 67, col.9 line 43 to col.10 line 11).

As per claim 31, wherein the first data includes for each software application an identification of associated data fields and characteristics of entitlements of users to each data field (col.7 line 60 to col.8 line 67, col.9 line 43 to col.10 line 11).

As per claim 32, further comprising the steps of: correlating the first and second data to determine authorized data field operations, said authorized operations being those particular operations of each data field which are permitted to a specified user; and generating the message based on the query and the determination of authorized operations, wherein said query includes an identification of the particular user and of a predetermined data field (col.7 line 60 to col.8 line 67, col.9 line 43 to col.10 line 11).

As per claim 33, further comprising the steps of: storing proprietary data useful to the software application; and storing third data relating to accessibility of the proprietary data (col.7 line 60 to col.8 line 67, col.9 line 43 to col.10 line 64).

As per claim 34, further comprising the steps of: correlating the first, second and third data to determine authorized data accesses aid authorized data accesses being those particular data accesses of the proprietary data which are permitted to a specified user; and generating the message based on the query and the determination of authorized data accesses, wherein said query includes an identification of the particular user and of predetermined proprietary data (col.7 line 60 to col.8 line 67, and col.9 line 43 to col.10 line 64).

As per claim 35, further comprising the step off creating a log entry relating to the message if the message indicates instructions which prohibit the particular software application access to the function (col.9 line 26 to line 42).

As per claim 36, further comprising the step of: administering the first and second data by manipulating one or both of the first and second data according to which of a plurality of clients the plurality of users is associated with (col.7 line 60 to col.8 line 67, and col.9 line 43 to col.10 line 64).

As per claim 37, further comprising the step of: administering the first and second data by manipulating one or both of the first and second data according to the identity of a particular one of the users (col.7 line 60 to col.8 line 67, and col.9 line 43 to col.10 line 64).

As per claim 38, further comprising the step of: administering the first and second data by manipulating one or both of the first and second data according to which of a plurality of roles the plurality of users is associated with (col.7 line 60 to col.8 line 67, and col.9 line 43 to col.10 line 64).

As per claim 39, further comprising the step of: administering the first and second data by manipulating all the first data relating to a specific one of the software application (col.7 line 60 to col.8 line 67, and col.9 line 43 to col.10 line 64).

As per claim 40, further comprising the step of: administering the first and second data by manipulating all the first data relating to one of the plurality of the plurality of preset functions associated with the software application (col.7 line 34 to col.8 line 67, and col.6 line 30 to line 57).

As per claim 42, further comprising: a non-volatile data store indicating a hierarchical arrangement of the plurality of access levels, and wherein the rules checker is further configured to consult the data store when determining the authorization of that particular user (col.7 line 34 to col.8 line 67, and col.6 line 30 to line 57).

As per claim 43, wherein the auditing application is further configured to provide real-time data logging and retrieval (col.7 line 9 to line 23).

As per claim 44, wherein any updates to data within the relational database are performed in real-time and the rules checker is further configured to use the updated data (col.7 line 9 to line 51).

As per claim 45, wherein the particular software application is a simulation application, said Simulation application is configured to: provide in the query to the rules checker a simulated

user identity and a simulated secured resource identity; receive from the rules checker the message forwarded by the rules checker; and determine the entitlements of the simulated user to access the simulated secured resource (col.6 line 30 to col.8 line 26).

As per claim 46, wherein the query requests a listing of entitlements for the one user, said listing identifying the entitlements for every application, function or proprietary data associated with the one user, and wherein the message includes said listing (col.6 line 30 to col.8 line 26).

As per claim 47, wherein query includes filtering parameters such that the listing includes only those entitlements which satisfy the filtering parameters (col.6 line 30 to col.8 line 26).

As per claim 48, wherein the filtering parameters specify one or more of a user role, a function identity, an application identity, a user identity, and a data access level (col.6 line 30 to col.8 line 26).

As per claim 49, wherein the authorization of the particular user to access proprietary data depends, at least in part, on the particular software application identity (col.6 line 30 to col.8 line 26).

As per claim 50, wherein the authorization of the particular user to access proprietary data depends, at least in part, on the particular function identity (col.6 line 30 to col.8 line 26).

As per claim 51, wherein the one of the users utilizes a remote system to access the particular function of the particular software application, and is not signed on to the operating system based on which the rules checker operates (col. 4 line 20 to line 50).

As per claim 52, wherein: the one of the users is an organization; and the second data specifies entitlements of the organization to access one or more functions of the particular software application, and entitlements of at least one individual user in the organization to access

at least one of the one or more functions of the particular software application that the organization is entitled to access (col.6 line 30 to col.8 line 26).

As per claim 54, wherein more than one hierarchical structure is provided, each of the more than one hierarchical structure is associated with a function of the organization, an organization structure of the organization, or geographical regions (Fig. 1, col.4 line 20 to line 58).

As per claim 55, wherein the access level is assigned to the individual user based on the individual user's role within the organization or the individual user's job function (col. 6 line 30 to col.8 line 67).

As per claim 56, wherein: the one of the users is an organization having associated proprietary data; and the second data specifies an authorization granted to an individual user of the organization to access at least part of the proprietary data associated with the organization, based on a function to be performed by the individual user (col. 6 line 30 to col.8 line 67).

As per claim 57, wherein the message includes that one user's authorized action on the at least one field, or the appearance of the at least one field to that one user (col.6 line 30 to line 57, and col.7 line 45 to line 60).

As per claim 58, wherein the entitlements of the plurality of users are dynamically configurable without the need to have a specific user to sign-off and sign-on again (col.9 line 26 to line 43).

As per claim 59, wherein the one of the users is an organization; and the second data specifies entitlements of the organization to access one or more functions of the particular software application, and entitlements of a role of the organization to access at least one of the

one or more functions of the particular software application that the organization is entitled to access; and a least one individual user of the organization is assignable to the role (col.9 line 26 to col.10 line 11).

As per claim 61, further comprising an auditing application configured to output information indicating that the query relates to a user that is not entitled to access the function of the software application (col.9 line 26 to col.10 line 12).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SYED ZIA whose telephone number is (571)272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

sz
July 7, 2008
/Syed Zia/
Primary Examiner, Art Unit 2131